TESTIMONY OF

PAUL ROSENZWEIG

SENIOR LEGAL RESEARCH FELLOW
CENTER FOR LEGAL AND JUDICIAL STUDIES

THE HERITAGE FOUNDATION[*]

214 MASSACHUSETTS AVENUE, NE
WASHINGTON, DC 20002

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION AND CYBERSECURITY

REGARDING

IMPROVING PRE-SCREENING OF AVIATION PASSENGERS AGAINST TERRORIST AND OTHER WATCH LISTS

29 JUNE 2005

[*] The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During 2004, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2004 income came from the following sources: Individuals 56%; Foundations 24%; Corporations 4%; Investment Income 11%; Publication Sales and Other 5%. The top five corporate givers provided The Heritage Foundation with 2% of its 2004 income. The Heritage Foundation's books are audited annually by the national accounting firm of Deloitte & Touche. A list of major donors is available from The Heritage Foundation upon request. Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

.

Good morning Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to testify before you today on the challenge of maintaining the balance between security and constitutionally protected freedoms inherent in responding to the threat of terror, in the particular context of the Transportation Security Administration's (TSA's) proposed Secure Flight system.

For the record, I am a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation, a nonpartisan research and educational organization. I am also an Adjunct Professor of Law at George Mason University where I teach Criminal Procedure and an advanced seminar on White Collar and Corporate Crime and I serve on the Editorial Board of the Journal of National Security Law and Policy.

I am a graduate of the University of Chicago Law School and a former law clerk to Judge R. Lanier Anderson of the U.S. Court of Appeals for the Eleventh Circuit. For much of the first 13 years of my career I served as a prosecutor in the Department of Justice and elsewhere, prosecuting white-collar offenses. During the two years immediately prior to joining The Heritage Foundation, I was in private practice representing principally white-collar criminal defendants. I have been a Senior Fellow at The Heritage Foundation since April 2002.

I should also note that I serve as Chairman of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. This group is constituted to advise the Secretary and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, as well as data integrity, data interoperability and other privacy-related issues.

Nothing in my testimony, oral or written, reflects the views of the Privacy Advisory Committee or any other member of the Committee. My own views, however, are certainly informed by my service on that Committee and the information I learn there. We heard testimony earlier this month, for example, at a hearing in Boston, about many of the Department's screening programs, including Secure Flight.

More broadly, my perspective on the question before you is that of a lawyer and a prosecutor with a law enforcement background, not that of technologist or an intelligence officer/analyst. I should hasten to add that much of my testimony today is based upon a series of papers I have written (or co-authored) on various aspects of this topic and testimony I have given before other bodies in Congress, all of which are available at The Heritage Foundation website (www.heritage.org). For any who might have read portions of my earlier work, I apologize for the familiarity that will attend this testimony. Repeating myself does have the virtue of maintaining consistency -- I can only hope that any familiarity with my earlier work on the subject does not breed contempt.

* * * * *

In this testimony, I want to do four things: summarize the history of the Secure Flight program; discuss the anticipated utility of Secure Flight and the most controversial aspect of its architecture, the possible use of commercial data to verify identity; discuss privacy impact compliance as a necessary condition for implementation; and finally, discuss the question of redress.

I. A Bit of History

One common critique offered by skeptics of new initiatives to combat terrorism is the concern that advances in information technology will unreasonably erode the privacy and anonymity to which American citizens are entitled. They fear, in effect, the creation of an "electronic dossier" on every American. Attention to this issue has particularly focused on TSA's proposal to use an enhanced information technology program to screen airplane passengers. That program, known as Secure Flight, is intended to identify every passenger to determine his or her presence on a watch list for screening or to be denied access to the plane.

Since September 11th, the aviation industry has undergone many changes to strengthen airport security. The TSA was created and placed in charge of passenger and baggage screeners (who are now federal employees). It has been using explosives detection systems on 90 percent of checked baggage and substantially expanded the Federal Air Marshal Service. However, little has been done to determine whether a person seeking to board an aircraft belongs to a terrorist organization or otherwise poses a threat. In order to meet this objective, the Transportation Security Administration is developing the Secure Flight.

Most of the changes made in airport security have focused on looking for potential weapons (better examination of luggage, more alert screeners) and creating obstacles to the use of a weapon on an aircraft (reinforced cockpit doors, armed pilots, etc). A computer-aided system would improve the TSA's ability to assess the risk a passenger may pose to air safety.

CAPPS I: The original, limited CAPPS I system was first deployed in 1996 by Northwest Airlines. Other airlines began to use CAPPS I in 1998, as recommended by the White House Commission on Aviation Safety and Security (also known as the Gore Commission).[1] In 1999, responding to public criticism, the FAA limited the use of CAPPS I – using it only to determine risk assessments for checked luggage screening. In other words, between 1999 and September 2001 CAPPS I information was not used as a basis for subjecting passengers to personal searches and questioning – only for screening checked bags. As a consequence even if CAPPS I flagged a high-risk passenger he could not be singled out for more intensive searches.

After September 11 CAPPS I returned to its original conception and is now again used to screen all passengers along with their carry-on and checked luggage. However, the criteria used to select passengers, such as last-minute reservations, cash payment, and short trips are over inclusive. This is a very crude form of pattern-recognition analysis. So crude that it can flag up to 50% of passengers in some instances, mainly in short haul markets.[2] These criteria are also widely known and thus readily avoided by any concerted terrorist

[1] *See* White House Commission on Aviation Safety and Security (Feb. 12, 1997) (available at http//www.airportnet.org/depts/regulatory/gorefinal.htm).

[2] *See* Robert W. Poole, Jr. & George Passatino, "A Risk-Based Airport Security Policy" Reason Public Policy Institute at 11 (May 2003).

effort. Nor does CAPPS I attempt to determine whether or not the federal government has information that may connect a specific perspective passenger with terrorism or criminal activity that may indicate they are a threat to the flight. And it is costly – I've heard informal estimates as high as $150 million per year for domestic airlines to operate the system. As a result, we are wasting resources: it's likely that if Osama bin Laden tried to board a plane today CAPPS I would not identify him for arrest or further inspection.[3]

The Current System: In the immediate aftermath of September 11 it quickly became obvious that the failure to make any matching effort was problematic. The existing watch lists were disjointed and inconsistent and could not be effectively shared with airlines (for fear of disclosing sensitive or confidential national security information). But some watch list matching was, rightly, deemed necessary.

To meet that perceived need the Administration took two steps. First, it created the Terrorist Screening Center in an effort to consolidate and coordinate the multiple government-wide watch lists. Second, the Administration created a system whereby watch list names were shared with individual airlines for them to match against their own customer lists.

This current system is problematic for several reasons:

- Most saliently, because of the national security sensitivity of the watch lists only a portion of the lists can be shared;
- Because each airline administers the watch list matching differently, there is no single common standard for defining a watch list "match";
- Because each airline uses different automated matching programs, there is a high variability in the matching operational methodology; and
- Because of differing programs and standards a list of "cleared" passengers who are on the watch list cannot be readily propagated throughout the system (no doubt the cause, for example, of Senator Kennedy's persistent screening).

Recognizing the inadequacy of the system and the waste of resources that attends the disutility of screening those who do not need to be screened, TSA began developing potential replacement systems. In the post-9/11 world the question is not really whether we will watchlist match, but how best to do it.

CAPPS II Proposed: The TSA reasonably believes that screening what a passenger is carrying is only part of the equation and began developing CAPPS II as a successor to

[3] It has been reported that the CAPPS I system was partially effective, flagging nine of the 19 September 11 terrorists for additional screening. *See* National Commission on Terrorist Attacks Upon the United States, "The Aviation Security System and the 9/11 Attacks: Staff Statement No. 3" (Jan. 27, 2004) (available at http://www.9-11commission.gov/hearings/hearing7/staff_statement_3.pdf]); *see also* Sara Goo and Dan Eggen, "9/11 Hijackers Used Mace and Knives, Panel Reports," Wa. Post at A1 (Jan. 28, 2004) (summarizing report). To the extent that is true it emphasizes both that some form of screening can be effective, that the limitation to bag-only screening was unwise, and that however effective electronic screening might be, the human element will always be a factor in insuring the success of any system.

CAPPS I in order to determine whether the individual poses a threat to aviation security. CAPPS II was intended to use government intelligence and law enforcement information in order to assign risk levels to passengers based on real information not arbitrary models. The TSA would then be able to devote more of its resources to those with a higher score (indicating they pose a greater risk), than those deemed to be a lesser concern (although some degree of randomness will need to be retained).

In January 2003, TSA released a Privacy Act notice for CAPPS II, the successor to CAPPS I.[4] Many critics raised substantial concerns. Some thought that CAPPS II, as originally proposed, was too broad in scope and could infringe on passengers' privacy. Others were concerned that the government should not rely on potentially flawed commercial data to prevent individuals from traveling by air. Some asserted that the use of knowledge discovery technologies on a wide variety of personal data could pose privacy and civil liberty violations. Finally, many wondered if individuals would be able to challenge their score.

In August 2003, TSA made available an Interim Final Privacy Notice on CAPPS II, which included substantial modifications to the initial proposal based on many of the concerns voiced in response to the first Privacy Notice.[5]

Under the Interim Notice, TSA would not keep any significant amount of information after the completion of a passenger's itinerary. Furthermore, TSA promised to will delete all records of travel for U.S. citizens and lawful permanent residents a certain number of days after the safe completion of the passenger's travels (7 days is the current anticipation). TSA also committed to developing a mechanism by which a passenger targeted for more thorough screening can seek to set the record straight if they think they have been identified in error.

More importantly, the CAPPS II system addressed privacy concerns by severely limiting the types of private information collected and the way in which commercial data will be examined. The proposed CAPPS II system would have accessed only a "passenger name record" (PNR), which includes information collected at the time the passenger makes the reservations, prior to the flight. Selected PNR information (including name, address, date of birth, and telephone number) was to be transmitted to commercial data providers for the sole purpose of authenticating the passenger's identity. This process would be similar to the credit card application procedure used to check for fraudulent information.

Secure Flight – In 2004, TSA again modified its pre-screening program, now renaming it Secure Flight. According to a Privacy Impact Assessment and Systems of Records Notice published in September 2004, the principal difference between Secure Flight and CAPPS II was to further tighten the privacy protections and to split into two distinct pieces the operational components of the system.[6] One part of the system would match PNR data to existing Terrorist (and other "no-fly") watch lists. The second part would test whether the fidelity of PNR data (that is the clarity with which the data unambiguously identifies a single unique individual) could be enhanced through the use of commercial data

[4] *See* 68 Fed. Reg. 2101 (Jan. 15, 2003).

[5] *See* 68 Fed. Reg. 45265 (Aug. 1, 2003).

[6] 69 Fed. Reg. 57345 (SORN), 57352 (PIA) (Sept. 24, 2004).

bases.[7] Consistent with those notices, and with the Congressional mandate to do so,[8] Secure Flight began a test of its system using historical data from June 2004 provided under order by the airlines.

The results of this testing have not yet been fully disclosed. In public remarks, however, TSA representatives have stated that the watch list matching portion of the project appears to have worked well, both in effectively matching PNR data with watch list information and in stress testing to demonstrate that the system is capable of handling the volume of inquires anticipated.

The best estimate is that after automated clearances, carriers operating independently have approximately a 2% "close" match rate – that is a rate that requires further inquiry and human intervention. This means that, on average there are 35,000 matches per day (assuming an average of 1.8 million travelers each day. Preliminary results suggest that with an "in-house" matching system run by TSA and with the addition of only the date of birth of an individual, this close match rate can be reduced by 60% to 0.8% of the travelling public – an average of 14,000 matches each day. If so, this will be a substantial improvement – and the use of commercial data has the potential to drive the number even lower, though testing is still ongoing.

Controversy has arisen regarding the program in the past few weeks, however, concerning its compliance with the original System of Records Notice (SORN) published in the Federal Register. The deviation was sufficiently great that TSA recently amended the notice of the scope of the system of records. In the original SORN[9] the system included only PNRs; information from the Terrorist Screening Center (TSC); authentication scores and codes from commercial data providers; and the results of comparisons between individuals identified in PNRs and the TSC watch list. The revised SORN,[10] issued last week, adds two new categories of information held in the system of records:

> PNRs that were enhanced with certain information obtained from commercial data – full name, address, date of birth, gender – and that were provided to TSA for purposes of testing the Secure Flight program; [and]
>
> Commercial data purchased and held by a TSA contractor for purpose of comparing such data with June 2004 PNRs and testing the Secure Flight program.

[7] A more detailed summary of the differences between CAPPS II and Secure Flight can be found in GAO, Secure Flight Development and Testing Under Way but Risks Should Be Managed as System is Further Developed, at Table 3 (GAO-05-356, March 2005).

[8] In the Intelligence Reform and Terrorism Prevention Act of 2004, Congress mandated testing of a passenger pre-screening program. *See* IRTPA, Pub. L. No. 108-458, § 4012, 118 Stat. 3638, 3714-19 (2004) (TSA directed to "commence testing of an advanced passenger prescreening system . . . utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government").

[9] 69 Fed. Reg. 57345 (Sept. 24, 2004).

[10] 70 Fed. Reg. 36319 (June 22, 2005).

The Privacy Officer has announced an investigation of Secure Flight to examine whether the actions which necessitated the modification of the SORN constituted a violation of Departmental privacy polices or law.

II. Secure Flight and Commercial Data

Why Secure Flight? -- The Secure Flight program poses some interesting and challenging problems in adapting the law to new technology and the realities of new technology to the law. First, if Secure Flight is to be effective its hallmark will be the idea that some form of "result" will necessarily be immediately available to TSA screeners on a "real-time" basis so that they can make near-instantaneous decisions regarding whom to screen or not screen prior to allowing passengers to board the aircraft. If Secure Flight were designed so that detailed personal information on each passenger were transmitted to every TSA screener, all would agree that the architecture of the system did not adequately protect individual privacy. The analysis passed by the Secure Flight system to TSA employees at the airport must be (and under current testing plans, will be) limited to a reported color code – red, yellow or green – and should not generally identify the basis for the assignment of the code.

Thus, Secure Flight proposes to precisely reverse the privacy protection equation being developed in other contexts. To protect privacy, other information technology program disaggregate analysis from identity by making the data available to the analyst while concealing the identity of the subject of the inquiry unless and until disclosure is warranted. In the reverse of this paradigm, Secure Flight will disclose the identity of the potential threat (through a red/yellow/green system displayed to the screener, warning of a particular individual) but will conceal from the screener the data underlying the analysis – at least until such time as a determination is made that the two pieces of information should be combined. The privacy protection built into Secure Flight is therefore the mirror image of the more common system. It is by no means clear which method of protecting privacy is *ex ante* preferable – but it is clear that the two systems operate differently and if we are to have any sort of Secure Flight system at all, it can only have privacy protections of the second kind.

Nor is Secure Flight necessarily a decrease in privacy. Rather, it requires trade-offs in different types of privacy. It substitutes one privacy intrusion (into electronic data) for another privacy intrusion (the physical intrusiveness of body searches at airports). It will allow us to target screening resources, while actually *reducing* the number of intrusive searches: Currently 14% of the traveling public are subject to some form of secondary screening. Secure Flight may reduce that to as low as 4% selected for additional screening.[11] More importantly, Secure Flight will also have the salutary effect of reducing the need for random searches and eliminate the temptation for screeners to use objectionable characteristics of race, religion, or national origin as a proxy for threat indicators.[12] For

[11] *See* Transcript of Media Roundtable with DHS Under Secretary Asa Hutchinson (Feb. 12, 2004) (available at www.tsa.gov).

[12] Some purely random searches will need to be retained in order to maintain the integrity of the inspection system and defeat so-called "Carnival Booth" attacks (named after a student algorithm proposing a method of defeating CAPPS). Adding a random factor to the inspection regime answers the problem. *See* Samidh Chakrabati & Aaron Strauss, "Carnival Booth: An Algorithm for Defeating the Computer-assisted Passenger Screening," (available at

many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy, fewer random searches, and a reduction in invidious racial profiling.

Finally, and perhaps most saliently, Secure Flight is a useful idea because it will allow us to focus scarce resources. One of the truly significant improvements in homeland security has come from the use of risk assessment and risk management techniques to identify salient threats and vulnerabilities and target resources (like inspectors) at those situations where the threats and vulnerability are greatest. Thus, rather than attempt fruitlessly to search every container entering the United States, we use information about the shipper, place of origin and other factors to select for inspection containers about which there is some ambiguity or concern. So, too, with Secure Flight – we can envision the day when TSA inspectors (and other resources such as Air Marshals), are allocated in the way we think best addresses actual risks of harm, increasing the chances of catching terrorists and minimizing the unnecessary intrusion into people's lives at times and places where there is no risk at all. Should Congress have any concerns at all about the intrusiveness of individual screening it should, at a minimum, recognize the utility of enhanced risk assessment technology.[13] To fail to do so would be even worse than our current system.

Which brings us to the final question of effectiveness. Of course, before full deployment, Secure Flight needs to demonstrate that it can work. It holds great promise – but promise is far different from reality. Thus, the ultimate efficacy of the technology developed is a vital antecedent question. If the technology proves not to work—if, for example, it produces 95 percent false positives in a test environment—than all questions of implementation may be moot. For no one favors deploying a new technology—especially one that impinges on liberty—if it is ineffective. Thus, Congress is right to insist that Secure Flight be thoroughly tested. Conversely, we are unwise to reject it before knowing whether the effectiveness problem can be solved.

Some critics are skeptical that Secure can ever work, characterizing it as the search for a "silver bullet" that cannot function because of Bayesian probability problems.[14] That broad statistical criticism is rejected by researchers in the field who believe that because of the high correlation of data variables that are indicative of terrorist activity, a sufficient number of variables can be used in any model to create relational inferences and substantially reduce the incidence of false positives.[15] And, in other environments, enhanced technology allowing the correlation of disparate databases and information has proven to have

http://www.swiss.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm) (describing program); K.A. Taipale, "Data Mining and Domestic Security," 5 COLUM. SCI. & TECH. L. REV. 2, at n.285 (2003) (explaining how addition of random screening guards against such attacks).

[13] Risk assessment need not be used only to identify particular individual activity. We could also imagine a world in which Secure Flight were used only to identify resource allocation methods – surging TSA resources, for example, to at-risk flights or airports without particularly singling out an individual for distinct scrutiny.

[14] *E.g.* Jeffrey Rosen, The Naked Crowd 105-06 (Random House 2004).

[15] *See* Remarks, David Jensen, "Data Mining in the Private Sector," Center for Strategic and International Studies, July 23, 2003; David Jensen, Matthew Rattigan, Hannah Blau, "Information Awareness: A Prospective Technical Assessment," SIGKDD '03 (August 2003) (ACM 1-58113-737-0/03/0008).

potentially significant positive uses. American troops in Iraq, for example, use the same sorts of link and pattern analysis, prediction algorithms and enhanced database technology that would form a part of Secure Flight to successfully track the guerrilla insurgency.[16]

It is also important to realize that there may be potentially divergent definitions of "effectiveness." Such a definition requires *both* an evaluation of the consequences of a false positive *and* an evaluation of the consequences of failing to implement the technology. If the consequences of a false positive are relatively modest (e.g. enhanced screening), and if the mechanisms to correct false positives are robust (as recommended below), then we might accept a higher false positive rate precisely because the consequences of failing to use Secure Flight technology (if it proves effective) could be so catastrophic. In other words, we might accept 1,000 false positives if the only consequence is heightened surveillance and the benefit gained is a 50 percent chance of preventing the next terrorist flight attack. The vital research question, as yet unanswered, is the actual utility of the system and the precise probabilities of its error rates.[17]

Commercial Data – One part of the efficacy answer lies in the question of the use of commercial data to disambiguate and resolve identities. Clearly, it is plausible to believe that the incidence of false positives can be reduced by the use of commercial data. Credit granting institutions do it all the time. Thus, in theory, there ought to be no reason why reliance on commercial data to enhance efficacy should be ruled out of bounds.

Indeed, if using commercial data works to reduce the unnecessary screening of correctly identified individuals it will have the salutary effect of enhancing privacy. We need, of course, to test this aspect of Secure Flight as well to insure that it works, but if it does and if it can be implemented in privacy-protective ways, then identity verification should be welcomed, not opposed

The question then, is whether it can be done in a manner that is sufficiently privacy protective. The outlines for such a privacy-protective system can be seen in the original SORN issued for the Secure Flight testing phase. Most notably, that SORN limited the Secure Flight system of records to authentication scores and codes provided by commercial data providers – in other words, the actual data that forms the basis for the authentication score would remain with the commercial database and not be transmitted to TSA.

[16] *See* AP, "Computer-sleuthing aids troops in Iraq," (Dec. 23, 2003). Any who doubt that, in some form, enhanced information search technology can work need only contemplate the recent arrest of LaShawn Pettus-Brown, whose date identified him as a fugitive when she "Googled" him. *See* Dan Horn, "Fugitive Done in by Savvy Date and Google," USA Today (Jan. 29, 2004) (available at http://www.usatoday.com/tech/news/2004-01-29-google-bust_x.htm). Compare that with the pre-September 11 prohibition (eliminated by the new FBI guidelines) on the FBI's use of Google. *See* L. Gordon Crovitz, "Info@FBI.gov," Wall St. J. (June 5, 2002). At some fundamental level the ultimate question is how to reconcile readily available technology in commercial and public use, with the broad governmental monopoly on the authorized use of force. Whatever the proper resolution, we cannot achieve it by hiding our heads in the sand and pretending that data integration technology does not exist.

[17] One final note – though privacy advocates are concerned about the false positives, the existence of an available system also may create civil tort liability for the failure to deploy. It is not fanciful to imagine tort suits against airlines that either do not implement Secure Flight or refuse to cooperate with TSA if by doing so they give rise to a false negative.

In my judgment, that system architecture strikes the right balance. It allows Secure Flight to take advantage of the commercial authentication methodology while minimizing the risk of governmental misuse of commercial data. It should be the cornerstone of a broader oversight structure to guard against abuse, which would include additional components along the following lines:

Though the details would need, of course, to be further developed, the outline of such an oversight system might include some or all of the following components:

- Secure Flight should be constructed to include an audit trail so that its use and/or abuse can be reviewed;
- It should not be expanded beyond its current use in identifying suspected terrorists and threats to national security – it should not be used as a means, for example, of identifying drug couriers or deadbeat dads;[18]
- The program should sunset after a fixed period of time, thereby ensuring adequate Congressional review;
- Secure Flight authorization should have significant civil and criminal penalties for abuse;
- The "algorithms" used to screen for potential danger must, necessarily, be maintained in secret, as their disclosure would frustrate the purpose of Secure Flight. They must, however, also be subject to appropriate congressional scrutiny in a classified setting and, if necessary, independent (possibly classified) technical scrutiny;
- As outlined below, there must be an adequate redress procedure in place;
- Because commercial databases may contain errors, no American should be totally denied a right to travel (i.e. red-carded) and subject to likely arrest as a suspected terrorist solely on the basis of public, commercial data. An indication of ambiguous identification and lack of authentication should form the basis only for enhanced screening. Adverse consequences of arrest or detention should only be based on intelligence from non-commercial sources.
- The No-Fly/Red Card designation, though initially made as the product of a computer algorithm, should never transmitted to the "retail" TSA screening system until it has been reviewed and approved by an official of sufficiently high authority within TSA to insure accountability for the system.[19]

In my view, the recent controversy over commercial data provides an important lens through which to view the Secure Flight program. Evidently (though, of course, the facts are not yet know) TSA needed to enhance PNR data with commercial data in order to

[18] *Cf.* William Stuntz, "Local Policing After the Terror," 111 Yale L. J. 2137, 2183-84 (2002) (use of expanded surveillance authority to prosecute only terrorists and other serious offenses).

[19] This would mirror the view of the European Union which styles it as a "right" to have human checking of adverse automated decisions. The EU Directives may be found at http://www.dataprivacy.ie/6aii-2.htm#15.

resolve residual identification ambiguities. This suggests, albeit indirectly, that the thesis of Secure Flight – that PNR data alone is sufficient to allow it to function – may be untenable. For the enhanced PNRs would probably not have been sought had they not been necessary. It also raises the question of whether the system's chosen architecture is the best – or whether in light of the necessity for enhancing PNRs we might not prefer a decentralized system.

But those questions are relatively technical in nature and, it seems, capable of resolution. The most significant aspect of the recent controversy is one of public perception. To that I now turn.

III. Compliance and the Privacy Act

Most Americans recognize the need for enhanced aviation security. They are even willing to accept certain governmental intrusions as a necessary response to the new threats.

But what they insist upon – and rightly so – is the development of systemic checks and balances to ensure that new authorities and powers given the government are not abused. And to achieve a suitable system of oversight, we need adequate transparency. We do not seek transparency of government functions for its own sake. Without need, transparency is little more than voyeurism. Rather, its ground is oversight – it enables us to limit the executive exercise of authority. Paradoxically, however, it also allows us to empower the executive; if we enhance transparency appropriately, we can also comfortably expand governmental authority, confident that our review of the use of that authority can prevent abuse. While accommodating the necessity of granting greater authority to the Executive branch, we must also demand that the executive accept greater review of its activities.

In that spirit, the Privacy Impact Assessments and Systems of Records Notices published by institutional actors like TSA serve several important functions. They define the program, they provide the opportunity for notice and comment on the program by the public and, most significantly, they provide a metric against which to measure the program's implementation. Prior notice of governmental activity is the hallmark of accountability – it fixes in time and place the ground for decision making and prevents *ex post* justifications from being developed.

Thus, we should be at least somewhat concerned by the recent revision of Secure Flights notice regarding the system of records being maintained. As I said earlier, the original SORN developed the right theoretical methodology for accessing commercial data for identify verification – maintaining the data in private hands and reporting the government only an authentication score. The most notable change identified in the new SORN issued last week is the breakdown in this screening methodology paradigm. To be sure, that change may prove to be a technical necessity – but if so, it is a change that ought to be publicly disclosed and debated before it is made. The fundamental premise of my analysis of Secure Flight (and indeed the analysis of all supporters and opponents) is that what is described in the TSA's privacy act notices is an accurate description of what is planned and what has happened. It undermines the transparency of the program and public confidence when that premise is proven wrong.

IV. Redress

Finally, the subject matter of the Secure Flight system calls for heightened sensitivity to the potential for an infringement on protected constitutional liberties. While Secure

Flight will not directly affect personal physical liberty, which lies at the core of constitutional protections, it does implicate at least one fundamental liberty interest guaranteed by the Constitution. Since the 1960s the Supreme Court has recognized a fundamental right to travel[20] – indeed, one might reasonably say that one purpose of the Federal union was to insure the freedom of commerce and travel within the United States.

Thus, there is a risk that a poorly designed system will unreasonably impinge upon a fundamental constitutional liberty. The risk of such impingement should not result in abandonment of the program – especially not in light of the potentially disastrous consequences of Type II error if there is another terrorist attack in the United States. However, we will need stringent oversight to provide the requisite safeguards for minimizing infringements of civil liberty in the first instance and correcting them as expeditiously as possible.

Any appropriate redress mechanism will need to solve two inter-related yet distinct problems. *First*, it will need to accurately and effectively identify false positives without creating false negatives in the process. For though we know that any watch list system will make mistakes by wrongly singling out an individual for adverse consequences, we also know that a watch list system may err by failing to correctly identify those against whom adverse consequences are warranted. And we also know that any redress mechanism must be as tamper-proof and spoof-proof as possible, for it is likely that those who are correctly placed on a terrorist watch list will use any redress process available to falsely establish that they should not be subject to enhanced scrutiny.

Second, any redress mechanism must effectively implement the requisite corrective measures. Already we have seen situations in which acknowledged "wrongly matched" errors in watch list systems cannot be readily corrected because of the technologically unwieldy nature of the information systems at issue. Even when TSA has recognized that a given person (for example, Senator Edward Kennedy) is repeatedly wrongly matched to a "no fly" list entry, correction proves challenging as one cannot just remove the more ambiguous watch list entry.[21] Thus, the legal, policy, and technological mechanisms must be built in to the watch listing system to allow for the effective handling of redress.

Sadly, the limitations of this forum prevent me from providing you a detailed of exactly what a system answering these questions would look like. But my colleague Jeff Jonas and I have written in detail about this question.[22] In short, we envision a system of third-party ombudsman-like review; initial administrative review; limitations on disclosure if necessary to accommodate national security concerns; a private cause of action to correct any permanent deprivation of liberty; and a system design requirement tethering and attributing information so that corrections propagate through the system rapidly. Our

[20] *Shapiro v. Thompson*, 398 U.S. 618 (1969).

[21] *See* Sara Goo, "Sen. Kennedy Flagged by No-Fly List,"*The Washington Post*, August 20, 2004, p. A1.. Others on the list, like Representative John Lewis, avoided secondary screening by including their middle initial. *See* Jeffrey McMurray, "Rep. Lewis says his name is on terrorist watch list," Associated Press, August 20, 2004.

[22] *See* Rosenzweig & Jonas, Correcting False Positives: Redress and the Watch List Conundrum, Legal Memorandum No. 17 (The Heritage Foundation, June 2005) (available at http://www.heritage.org/Research/HomelandDefense/lm17.cfm)

conclusion is that these questions are soluble – and that prior to full-scale implementation TSA must solve them.

* * * * *

In short, Secure Flight continues to have some significant issues that need to be addressed. But it also is a system of great promise. Failing to make the effort to use new technology wisely poses grave risks and is an irresponsible abdication of responsibility.

As six former top-ranking professionals in America's security services recently observed, we face two problems—both a need for better analysis and, more critically, "improved espionage, to provide the essential missing intelligence." In their view, while there was "certainly a lack of dot-connecting before September 11," the more critical failure was that "[t]here were too few useful dots."[23] Secure Flight technology can help to answer both of these needs. Indeed, resistance to new technology poses practical dangers. As the Congressional Joint Inquiry into the events of September 11 pointed out in noting systemic failures that played a role in the inability to prevent the terrorist attacks:

> 4. Finding: While technology remains one of this nation's greatest advantages, it has not been fully and most effectively applied in support of U.S. counterterrorism efforts. Persistent problems in this area included a lack of collaboration between Intelligence Community agencies [and] *a reluctance to develop and implement new technical capabilities aggressively* . . . .[24]

Or, as one commentator has noted, the reflexive opposition to speculative research by some is "downright un-American."[25] Though Secure Flight technology might prove unavailing, the only certainty at this point is that no one knows. It would be particularly unfortunate if Congress opposed basic research without recognizing that in doing so it was demonstrating a "lack [of] the essential American willingness to take risks, to propose outlandish ideas and, on occasion, to fail."[26] That flaw is the way to stifle bold and creative ideas—a "play it safe" mindset that, in the end, is a disservice to American interests.

Mr. Chairman, thank you for the opportunity to testify before the Subcommittee. I look forward to answering any questions you might have.

[23] Robert Bryant, John Hamre, John Lawn, John MacGaffin, Howard Shapiro & Jeffrey Smith, "America Needs More Spies," *The Economist*, July 12, 2003, p. 30.

[24] *Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001*, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, 107th Cong., 2nd Sess., S. Rept. No. 107–351 and H. Rept. No. 107–792, Dec. 2002, p. xvi (available at *http://www.fas.org/irp/congress/2002_rpt/911rept.pdf*) (emphasis supplied). The Joint Inquiry also critiqued the lack of adequate analytical tools, *id.* Finding 5, and the lack of a single means of coordinating disparate counterterrorism databases, *id.* Findings 9 & 10. Again, aspects of the CAPPS II program are intended to address these inadequacies and limitations on the research program are inconsistent with the Joint Inquiry's findings.

[25] *See* David Ignatius, "Back in the Safe Zone," *The Washington Post,* August 1, 2003, p. A19.

[26] *Id.*